UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/026,043	10/25/2001	Huayan A. Wang	1190	8635

7590 11/14/2007

Oleg F. Kaplun, Esq
FAY KAPLUN & MARCIN LLP
150 Broadway
Suite 702
New York, NY 10038

EXAMINER	
KIM, JUNG W	

ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
11/14/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/026,043	WANG ET AL.	
	Examiner	Art Unit	
	Jung Kim	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 September 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This Office action is in response to the RCE filed on 9/14/07.

2. Claims 1-21 are pending.

Continued Examination Under 37 CFR 1.11

3. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e); was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 8/31/07 has been entered.

Response to Arguments

4. Applicant argues that Leung as combined with Marko does not disclose the new limitation "determining if the particular access point has authentication data associated with the roaming device at the particular access point if the determination is positive, or carrying out the authentication process at the authentication server if the determination is negative" as recited in claim 1. In particular, applicant argues "the authentication of the mobile node in Leung can be performed either by the server which provides a plurality of security associations for a plurality of mobile nodes, or by the Home Agent ... where to perform the authentication is not triggered by any particular condition, such as

the Home Agent's determining if it has the authentication data associated with the mobile node, but is configured according to the preference of the network operator." (Remarks, pg. 9, 1st paragraph) Applicant's argument is not persuasive for the following reason: contrary to applicant's allegations, Leung suggests authenticating the mobile node at the authentication server if the particular access point does not have authentication data associated with the roaming device; otherwise, authenticating the mobile node at the particular access point. On col. 7:56-65, Leung discloses

> i. To reduce the effort associated with this, the security association may be **temporarily loaded** into memory (e.g., a portion of DRAM) of the Home Agent. In this manner, **some transfers** of security associations from the server to the Home Agent are eliminated. A suitable algorithm for clearing security associations from the Home Agent's memory may be employed (e.g., a least recently used (LRU) algorithm). While this approach can reduce traffic between server and Home Agent--and thereby eliminate attendant delay--it must also account for modifications of security associations (e.g., keys) on the server. [emphasis added]

5. In this portion of the Leung disclosure, the mobile station's authentication data is not permanently stored in the access point, rather it appears that the data is cached when the mobile station first authenticates with the authentication server via this particular access point. This notion of caching information after an initial retrieval is one of the fundamental concepts in memory management as known to one of ordinary skill in the art: the most recent information culled from memory is the most likely information to be requested on a subsequent request. By caching the information at a local station, memory access is reduced. In the case of Leung, when a mobile station first arrives at a base station where the base station has no authentication data corresponding with the mobile station, then the authentication data is retrieved from the authentication server;

the authentication data is then cached at the base station, and subsequent authentication can proceed locally at the base station. Hence, Leung in view of Marko discloses the limitation in question.

6. Applicant's remaining arguments are based on those arguments discussed above. Hence, the claims remain rejected under the prior art of record.

Claim Rejections - 35 USC § 103

7. Claims 1-3, 6, 10, 11 and 15-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Leung USPN 6,760,444 (hereinafter Leung) in view of Marko et al. USPN 5,732,350. (hereinafter Marko)

8. As per claim 1, Leung discloses a method for authenticating a roaming device with a network, comprising the steps of:

a. generating, by an authentication server of the network, authentication data associated with the roaming device (col. 7:35-36);

b. sending, by the authentication server, the authentication data to an access point of the network, the access point being connected to the authentication server(7:38-50); and

c. when the roaming device roams to a particular access point, determining if the particular access point has authentication data associated with the roaming device, using the authentication data to locally authenticate the roaming device at the particular access point if the determination is positive, or carrying out the

authentication process at the authentication server if the determination is negative. (7:50-67)

Leung does not disclose sending the authentication data to a plurality of access points and storing the authentication data in the plurality of access points, such that the roaming device is locally authenticated at a particular access point of the plurality of access points. Marko discloses a method for registering a mobile station among a plurality of base stations based upon a dynamic algorithm. When a mobile station approaches a cell where the mobile station is not yet registered, the mobile station registers with a based station in this cell, whereupon a network controller automatically registers the mobile station with all base stations within the group defined by the cell grouping level. Col. 7:24-57; 8:51-9:28. This enables the mobile station to roam among a cell grouping without registering each time the mobile moves to a new base station within the grouping. It would be obvious to one of ordinary skill in the art at the time the invention was made to send the authentication data to a plurality of access points and locally store the authentication data in the plurality of access points. One would be motivated to do so to reduce user registration traffic. Marko, col. 1:58-65; 2:36-40. The aforementioned covers the limitation of claim 1.

9. As per claim 2, the rejection of claim 1 under 35 U.S.C. 103(a) as being unpatentable over Leung in view of Marko is incorporated herein. In addition, the method further comprising the step of storing the authentication data in a memory arrangement of each of the access points. See Leung, col. 7:50-67; Marko, 7:24-56.

10. As per claim 3, the rejection of claim 1 under 35 U.S.C. 103(a) as being unpatentable over Leung in view of Marko is incorporated herein. Leung does not expressly teach the authentication data is encrypted. However, it is notoriously well known in the art that authentication data transmitted in the clear is susceptible to sniffing attacks. To prevent authentication data from being stolen, these values are typically encrypted using a shared secret between the sender and receiver. For example, in the RADIUS protocol, a password transmitted from a client to an authentication server is hidden using a shared secret. Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made for the authentication data to be transmitted securely to prevent the data from being stolen as known to one of ordinary skill in the art. The aforementioned cover the limitations of claim 3.

11. As per claim 6, the rejection of claim 1 under 35 U.S.C. 103(a) as being unpatentable over Leung in view of Marko is incorporated herein. In addition, the method further comprising the preliminary steps of determining if the particular access point has authentication data associated with the roaming device; if the determination is positive, proceed to the step of using the authentication data to locally authenticate the roaming device at the particular access point; and if the determination is negative, proceed to the step of generating, by an authentication server of the network, authentication data associated with the roaming device. Leung, col. 7:10-31; 7:56-8:8.

12. As per claim 10, Leung discloses a method for authenticating a roaming device with a network, comprising the steps of:

d. connecting the roaming device with an authentication server upon a contact of the roaming device with a first access point of the network; authenticating the roaming device with the authentication server if the access point has no authentication data associated with the roaming device; generating authentication data for the roaming device; distributing, by the authentication server, the authentication data to the first access point of the network; and locally authenticating the roaming device upon a contact with the first access point using the distributed authentication data. Col. 7:35-67.

Leung does not disclose sending the authentication data to a second access point and storing the authentication data in the second access point, then locally authenticating the roaming device upon a contract with the second access point using the distributed authentication data. Marko discloses a method for registering a mobile station among a plurality of base stations based upon a dynamic algorithm. When a mobile station approaches a cell where the mobile station is not yet registered, the mobile station registers with a based station in this cell, whereupon a network controller automatically registers the mobile station with all base stations within the group defined by the cell grouping level. Col. 7:24-57; 8:51-9:28. This enables the mobile station to roam among a cell grouping without registering each time the mobile moves to a new base station within the grouping. It would be obvious to one of ordinary skill in the art at the time the invention was made to send the authentication data to a second access point and store

the authentication data in the second access point, then locally authenticate the roaming device upon a contract with the second access point using the distributed authentication data. One would be motivated to do so to reduce user registration traffic. Marko, col. 1:58-65; 2:36-40. The aforementioned covers the limitation of claim 10.

13. As per claim 11, the rejection of claim 10 under 35 U.S.C. 103(a) as being unpatentable over Leung in view of Marko is incorporated herein. In addition, the method further comprising the step of authenticating the roaming device with the authentication server if the local authentication of the roaming device fails. Leung, col. 7:10-31; 7:56-8:8.

14. As per claim 15, the rejection of claim 10 under 35 U.S.C. 103(a) as being unpatentable over Leung in view of Marko is incorporated herein. In addition, the authentication server is a remote authentication dial-in user server. Leung, col. 7:1-5.

15. As per claim 16, Leung discloses a system for authenticating a roaming device with a network, comprising:

e. an authentication server connected to the network; and first and second access points connected to the authentication server, the first and second access points being capable of communicating with the roaming device, each of the first and second access points including a memory arrangement capable of storing

> authentication data corresponding to the roaming device, wherein the authentication server sends the authentication data to the first access point upon an initial authentication procedure of the roaming device with the first access point when the first access point has no authentication data associated with the roaming device, and wherein the first access point authenticates the roaming device upon a contact of the roaming device with the first access point. Col. 7:35-67.

Leung does not disclose sending the authentication data to a second access point and storing the authentication data in the second access point, then locally authenticating the roaming device upon a contract with the second access point using the distributed authentication data. Marko discloses a method for registering a mobile station among a plurality of base stations based upon a dynamic algorithm. When a mobile station approaches a cell where the mobile station is not yet registered, the mobile station registers with a based station in this cell, whereupon a network controller automatically registers the mobile station with all base stations within the group defined by the cell grouping level. Col. 7:24-57; 8:51-9:28. This enables the mobile station to roam among a cell grouping without registering each time the mobile moves to a new base station within the grouping. It would be obvious to one of ordinary skill in the art at the time the invention was made to send the authentication data to a second access point and store the authentication data in the second access point, then locally authenticate the roaming device upon a contract with the second access point using the distributed authentication data. One would be motivated to do so to reduce user registration

traffic. Marko, col. 1:58-65; 2:36-40. The aforementioned covers the limitation of claim 16.

16. As per claim 17, the rejection of claim 16 under 35 U.S.C. 103(a) as being unpatentable over Leung in view of Marko is incorporated herein. In addition, the second access point authenticates the roaming device with the authentication server if the authentication data is not found in the memory arrangement of the second access point. Leung, col. 7:10-31; 7:56-8:8.

17. As per claim 18, the rejection of claim 16 under 35 U.S.C. 103(a) as being unpatentable over Leung in view of Marko is incorporated herein. In addition, the second access point authenticates the roaming device with the authentication server if the local authentication of the roaming device at the second access point fails. Leung, col. 7:10-31; 7:56-8:8.

18. Claims 4 and 5 are rejected under 35 USC 103(a) as being unpatentable over Leung in view of Marko, and further in view of Ablay et al. USPN 5,408,683. (hereinafter Ablay)

19. As per claim 4, the rejection of claim 3 under 35 USC 103(a) as being unpatentable over Leung in view of Marko is incorporated herein. Leung does not expressly disclose using prediction algorithms to anticipate where the roaming device

will roam to determine to which access points to send the encrypted authentication data. Ablay discloses a method of tracking subscribers in a networked radio communications system having a plurality of trunked communication networks using location information of the subscribers to anticipate a roaming unit's location to reduce the number of registrations and de-registrations of the roaming unit. Col. 5:19-60; 6:26-57. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Ablay with the invention of Leung and Marko to use prediction algorithms to anticipate where the roaming device will roam to determine to which access points to send the encrypted authentication data. One would be motivated to do so to reduce the transmission overhead in keeping track of roaming subscribers. Ablay, 3:30-37. The aforementioned cover the limitations of claim 4.

20. As per claim 5, the rejection of claim 4 under 35 USC 103(a) as being unpatentable over Leung in view of Marko and Ablay is incorporated herein. In addition, the limitation of sending the encrypted authentication data to all the access points is an obvious enhancement in view of the teaching of Ablay that a mobile unit's registration is maintained at all access points in the anticipated probable locations of the mobile unit. Ablay, col. 5:19-26. The aforementioned cover the limitations of claim 5.

21. Claims 7, 8 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Leung in view of Marko, and further in view of Vij et al. USPN 6,452,910. (hereinafter Vij)

22. As per claim 7, the rejection of claim 6 under 35 U.S.C. 103(a) as being unpatentable over Leung in view of Marko is incorporated herein. (supra) In addition, the step of using the authentication data to locally authenticate the roaming device further comprises reassociating the roaming device with the particular access point of the access points by providing identification information. Leung, col. 7:10-13. However, Leung only discloses that the roaming device provides identification, and does not disclose that an exchange occurs between the roaming device and access points to reassociate. Vij discloses a management means for wireless access points wherein wireless devices are mutually authenticated with access points utilizing a common link key to verify that the wireless device is authorized to access the access point, and to ensure that the access point is the intended receiver. Col. 11:1-7. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the reassociating to include a mutual authentication between the roaming device and the access point, since it is desirous to verify that the participants belong to the same local network. Vij, ibid. The aforementioned cover the limitations of claim 7.

23. As per claim 8, the rejection of claim 7 under 35 U.S.C. 103(a) is incorporated herein. In addition, the reassociating step further includes the substeps of: searching a memory arrangement of the particular access point for the authentication data associated with the roaming device; and if the authentication data is found, performing a

mutual authentication procedure between the roaming device and the particular access point. Leung, col. 7:10-31; 7:56-8:8; Vij, 11:1-7.

24. As per claim 13, the rejection of claim 10 under 35 U.S.C. 103(a) as being unpatentable over Leung in view of Marko is incorporated herein. In addition, Leung discloses the locally authenticating step further includes the substeps of: providing identification data by the roaming device to the second access point; and correlating the identification data with the distributed authentication data. Col. 7:10-13. However, Leung only discloses that the roaming device provides identification, and does not disclose exchanging identification between the roaming device and access points to reassociate. Vij discloses a management means for wireless access points wherein wireless devices are mutually authenticated with access points using a common link key to verify that the wireless device is authorized to access the access point, and to ensure that the access point is the intended receiver. Col. 11:1-7. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the reassociating to include a mutual authentication between the roaming device and the access point, since it is desirous to verify that the participants of a transmission belong to the same local network. Vij, ibid. The aforementioned cover the limitations of claim 13.

25. Claims 9, 12 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Leung in view of Marko, and further in view of Zhang et al. US Patent Application

no. 20020174335 (hereinafter Zhang); RFC 2138 is incorporated to illustrate inherent properties of the RADIUS protocol.

26. As per claim 9, the rejection of claim 1 under 35 U.S.C. 103(a) as being unpatentable over Leung in view of Marko is incorporated herein. In addition, the generating step further includes the steps of: receiving an authentication request from the roaming device; determining that the roaming device can be granted access to network services. Leung, col. 7:11-8:12. Leung does not expressly teach generating an encrypted session key associated with the roaming device in the authentication server; wherein the authentication request is encrypted. Zhang discloses an authentication procedure for mobile devices designed by Cisco wherein a roaming user is authenticated via an access point, and uses the RADIUS protocol to authenticate the user to an authentication server. Upon, authentication, an encrypted session key is delivered from the authentication server to the access point and the user. (pg. 3, paragraphs 44-46; RFC 2138, pg. 4, last sentence, section 2, the password is encrypted using a method based on the RSA message digest algorithm MD5) Further, it is notoriously well known that authentication data transmitted in the clear is susceptible to sniffing attacks; to prevent authentication data from being stolen, these values are typically encrypted using a shared secret between the sender and receiver. For example, in the RADIUS protocol, a password transmitted from a client to an authentication server is hidden using a shared secret. Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made to generate an

encrypted session key associated with the roaming device in the authentication server; wherein the authentication request is encrypted. One would be motivated to do so to securely transmit data as reflected in the RADIUS protocol and the Cisco authentication procedure. The aforementioned cover the limitations of claim 9.

27. As per claims 12 and 14, the rejection of claim 10 under 35 U.S.C. 103(a) as being unpatentable over Leung in view of Marko is incorporated herein. In addition, Leung discloses the use of RADIUS protocol to authenticate the user with an authentication server, but Leung does not expressly disclose the distribution step further includes the substep of distributing an encrypted session key to the first and second access points, the method further comprising the steps of establishing a shared secret encryption between the authentication server and the first and second access points. Zhang discloses an authentication procedure for mobile devices designed by Cisco wherein a roaming user is authenticated via an access point, and uses the RADIUS protocol to authenticate the user to an authentication server. Upon, authentication, an encrypted session key is delivered from the authentication server to the access point and the user (pg. 3, paragraphs 44-46; RFC 2138, pg. 4, last sentence, section 2, the password is encrypted using a method based on the RSA message digest algorithm MD5) Further, it is notoriously well known that authentication data transmitted in the clear is susceptible to sniffing attacks; to prevent authentication data from being stolen, these values are typically encrypted using a shared secret between the sender and receiver. Hence, it would be obvious to one of ordinary skill in the art at the time the

invention was made for the distribution step to further include the substep of distributing an encrypted session key to the first and second access points, the method further comprising the steps of establishing a shared secret encryption between the authentication server and the first and second access points. One would be motivated to do so to securely transmit data as reflected in the RADIUS protocol and the Cisco authentication procedure. The aforementioned cover the limitations of claims 12 and 14.

28. Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Leung in view of Zhang; RFC 2138 is incorporated to illustrate inherent properties of the RADIUS protocol.

29. As per claim 19, Leung discloses a method for authenticating a roaming device with a network, comprising the steps of: with an authentication server, receiving an authentication request from a roaming device if the access point connected with the roaming device has no authentication data associated with the roaming device, sending the authentication data to an access point of the network, and utilizing the authentication data to authenticate the roaming device at the access point. Leung does not disclose the request being encrypted with a first shared code; generating a session key associated with the roaming device; sending the session key to an access point of the network, the session key being encrypted with a second shared code; and utilizing the session key to authenticate the roaming device at the access point, and to encrypt

data exchanged between the roaming device and the access point. Zhang discloses an authentication procedure for mobile devices designed by Cisco wherein a roaming user is authenticated via an access point, and uses the RADIUS protocol to authenticate the user to an authentication server. Upon, authentication, an encrypted session key is delivered from the authentication server to the access point and the user (pg. 3, paragraphs 44-46; RFC 2138, pg. 4, last sentence, section 2, the password is encrypted using a method based on the RSA message digest algorithm MD5) Further, it is notoriously well known that authentication data transmitted in the clear is susceptible to sniffing attacks; to prevent authentication data from being stolen, these values are typically encrypted using a shared secret between the sender and receiver. For example, in the RADIUS protocol, a password transmitted from a client to an authentication server is hidden using a shared secret. Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made for the request to be encrypted with a first shared code; generating a session key associated with the roaming device; sending the session key to an access point of the network, the session key being encrypted with a second shared code; and utilizing the session key to authenticate the roaming device at the access point, and to encrypt data exchanged between the roaming device and the access point. One would be motivated to do so to securely transmit data as reflected in the RADIUS protocol and the Cisco authentication procedure. The aforementioned cover the limitations of claim 19.

30. Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Leung in view of Zhang, and further in view of Marko.

31. As per claim 20, the rejection of claim 19 under 35 U.S.C. 103(a) is incorporated herein. Leung does not disclose the step of sending the encrypted session key to a further access point of the network to authenticate the roaming device at the further access point. Marko discloses a method for registering a mobile station among a plurality of base stations based upon a dynamic algorithm. When a mobile station approaches a cell where the mobile station is not yet registered, the mobile station registers with this station, whereupon a network controller automatically registers the mobile station with all base stations within the group defined by the cell grouping level. Col. 7:24-57; 8:51-9:28. This enables the mobile station to roam among a cell grouping without registering each time the mobile moves to a cell within the grouping. It would be obvious to one of ordinary skill in the art at the time the invention was made to include the step of sending the encrypted session key to a further access point of the network to authenticate the roaming device at the further access point. One would be motivated to do so to reduce user registration traffic. Marko, col. 1:58-65; 2:36-40. The aforementioned cover the limitations of claim 20.

32. Claim 21 is rejected under 35 U.S.C. 103(a) as being unpatentable over Leung in view of Zhang, and further in view of Quick, Jr. USPN 6,178,506 (hereinafter Quick '506).

33. As per claim 21, the rejection of claim 19 under 35 U.S.C. 103(a) is incorporated herein. In addition, Leung in view of Zhang discloses the method further comprising the steps of: generating a first key of the session key to perform authentication of the roaming device at the access point; and generating a second key of the session key to encrypt data exchanges between the roaming device and the access point. See Leung, 7:50-61; see Zhang, paragraph 45. Leung does not expressly teach the first key as being different from the second key. Quick '506 discloses an authentication method wherein a first portion of a session key is used for authentication and a second portion of the session key is used for encryption. Since, the session key is larger then the required byte size necessary for authentication, the portion not used for authentication is used for encryption. Col. 5:38-50. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the first key generated from the session key to perform authentication and the second key generated from the session key to perform encryption to be different keys, since the protocols for authentication and encryption typically require different length keys. Quick '506, 5:45-50. The aforementioned cover the limitations of claim 21.

Communications Inquiry

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W. Kim whose telephone number is 571-272-3804. The examiner can normally be reached on M-F 9:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jung W Kim
Examiner
Art Unit 2132

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100